Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of the Claims

1. (Currently Amended) A method performed by a user terminal of a wireless access network, the method comprising:

scrambling a user terminal certificate using a shared secret to be known only by the user terminal and an access point of the wireless access network, the scrambled user terminal certificate including a user terminal public key which corresponds to a user terminal private key; [[and]]

generating an authenticator string including data encrypted with the user terminal private key; and

sending a message to the access point, the message including the scrambled user terminal certificate and the authenticator string.

2. (Original) The method of claim 1, further comprising generating the shared secret and providing the shared secret to the access point.

3. (Currently Amended) The method of claim [[1]] 2, wherein providing the shared secret to the access point comprises ~~the message further including~~ encrypting the shared secret ~~encrypted~~ with an access point public key.

4. (Original) The method of claim 1, wherein scrambling the user terminal certificate using the shared secret comprises combining the user terminal certificate with a pseudo-random sequence generated by a linear feedback shift register initialized with a part of the shared secret.

5. (Original) The method of claim 4, wherein the part of the shared secret used to initialize the linear feedback shift register is not used for symmetric key cryptography between the user terminal and the access point.

6. (Original) The method of claim 5, wherein the remainder of the shared secret is used for symmetric key cryptography between the user terminal and the access point.

7. (Currently Amended) A user terminal comprising:

a memory to store a user terminal private key and a user terminal certificate, the user terminal certificate including a user terminal public key which corresponds to the user terminal private key;

a processor coupled to the memory to scramble the user terminal certificate using a shared secret to be known only by the user terminal and an access point of the wireless access network and to generate an authenticator string including data encrypted with the user terminal private key; and

a transmitter coupled to the processor to send a message to the access point, the message including the scrambled user terminal certificate and the authenticator string.

8. (Currently Amended) The user terminal of claim 7, wherein the processor [[is]] also [[to]] generates the shared secret and the transmitter [[is]] also [[to]] provides the shared secret to the access point.

9. (Currently Amended) The user terminal of claim [[7]] 8, wherein the transmitter provides the shared secret to the access point by encrypting ~~including in the message~~ the shared secret ~~encrypted~~ with an access point public key.

10. (Original) The user terminal of claim 7, wherein the processor scrambles the user terminal certificate using the shared secret by combining the user terminal certificate with a

pseudo-random sequence generated by a linear feedback shift register initialized with a part of the shared secret.

11. (Original) The user terminal of claim 10, wherein the part of the shared secret used to initialize the linear feedback shift register is not used for symmetric key cryptography between the user terminal and the access point.

12. (Original) The user terminal of claim 11, wherein the remainder of the shared secret is used for symmetric key cryptography between the user terminal and the access point.

13. (Currently Amended) A method performed by an access point of a wireless access network, the method comprising:

receiving a message from a user terminal of the wireless access network, the message containing a shared secret encrypted with an access point public key, an authenticator string including data encrypted with a user terminal private key, and a user terminal certificate scrambled using the shared secret, the scrambled user terminal certificate including a user terminal public key which corresponds to the user terminal private key;

decrypting the shared secret using an access point private key; [[and]]

unscrambling the user terminal certificate using the decrypted shared secret[[.]]; and

decrypting the authenticator string using the user terminal public key.

14. (Original) The method of claim 13, wherein unscrambling the user terminal certificate using the shared secret comprises combining the scrambled user terminal certificate with a pseudo-random sequence generated by a linear feedback shift register initialized with a part of the decrypted shared secret.

15. (Original) The method of claim 14, wherein the part of the decrypted shared secret used to initialize the linear feedback shift register is not used for symmetric key cryptography between the user terminal and the access point.

16. (Original) The method of claim 15, wherein the remainder of the shared secret is used for symmetric key cryptography between the user terminal and the access point.

17. (Canceled)

18. (Currently Amended) An access point comprising:

a receiver to receive a message from a user terminal, the message containing a shared secret encrypted with an access point public key, an authenticator string including data encrypted with a user terminal private key, and a user terminal certificate scrambled using the shared secret, the user terminal certificate including a user terminal public key which corresponds to the user terminal private key; and

a processor coupled to the receiver to decrypt the shared secret using an access point private key, [[and]] unscramble the user terminal certificate using the decrypted shared secret, and decrypt the authenticator string using the user terminal public key.

19. (Original) The access point of claim 18, wherein the processor unscrambles the user terminal certificate using the shared secret by combining the scrambled user terminal certificate with a pseudo-random sequence generated by a linear feedback shift register initialized with a part of the decrypted shared secret.

20. (Original) The access point of claim 19, wherein the part of the decrypted shared secret used to initialize the linear feedback shift register is not used for symmetric key cryptography between the user terminal and the access point.

21. (Original) The access point of claim 20, wherein the remainder of the shared secret is used for symmetric key cryptography between the user terminal and the access point.

22. (Canceled)

23. (Currently Amended) A machine-readable medium storing data representing instructions that, when performed by a processor of a user terminal, causes the processor to perform operations comprising:

scrambling a user terminal certificate using a shared secret to be known only by the user terminal and an access point of the wireless access network, the scrambled user terminal certificate including a user terminal public key which corresponds to a user terminal private key; [[and]]

generating an authenticator string including data encrypted with the user terminal private key; and

sending a message to the access point, the message including the scrambled user terminal certificate and the authenticator string.

24. (Original) The machine-readable medium of claim 23, wherein the instructions further cause the processor to perform operations comprising generating the shared secret and providing the shared secret to the access point.

25. (Currently Amended) The machine-readable medium of claim [[23]] 24, wherein providing the shared secret to the access point comprises encrypting ~~the message further including~~ the shared secret ~~encrypted~~ with an access point public key.

26. (Original) The machine-readable medium of claim 23, wherein scrambling the user terminal certificate using the shared secret comprises combining the user terminal certificate with

a pseudo-random sequence generated by a linear feedback shift register initialized with a part of the shared secret.

27. (Original) The machine-readable medium of claim 26, wherein the part of the shared secret used to initialize the linear feedback shift register is not used for symmetric key cryptography between the user terminal and the access point.

28. (Original) The machine-readable medium of claim 27, wherein the remainder of the shared secret is used for symmetric key cryptography between the user terminal and the access point.

29. (Currently Amended) A machine-readable medium storing data representing instructions that, when performed by a processor of an access point, causes the processor to perform operations comprising:

receiving a message from a user terminal of the wireless access network, the message containing a shared secret encrypted with an access point public key, an authenticator string including data encrypted with a user terminal private key, and a user terminal certificate scrambled using the shared secret, the scrambled user terminal certificate including a user terminal public key which corresponds to a user terminal private key;

decrypting the shared secret using an access point private key; [[and]]

unscrambling the user terminal certificate using the decrypted shared secret[[.]]; and

decrypting the authenticator string using the user terminal public key.

30. (Original) The machine-readable medium of claim 29, wherein unscrambling the user terminal certificate using the shared secret comprises combining the scrambled user terminal certificate with a pseudo-random sequence generated by a linear feedback shift register initialized with a part of the decrypted shared secret.

31. (Original) The machine-readable medium of claim 30, wherein the part of the decrypted shared secret used to initialize the linear feedback shift register is not used for symmetric key cryptography between the user terminal and the access point.

32. (Original) The machine-readable medium of claim 31, wherein the remainder of the shared secret is used for symmetric key cryptography between the user terminal and the access point.

33. (Canceled)